(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 26 783 A 1**

(51) Int. Cl.[7]:
H 04 L 9/32
H 04 L 12/16
H 04 N 1/44

(21) Aktenzeichen: 199 26 783.9
(22) Anmeldetag: 11. 6. 1999
(43) Offenlegungstag: 14. 12. 2000

(71) Anmelder:
Röhrhoff, Richard, 41061 Mönchengladbach, DE;
Brose, Peter, 41063 Mönchengladbach, DE

(74) Vertreter:
Kiani & Springorum Patent- u. Rechtsanwälte, 40213 Düsseldorf

(72) Erfinder:
gleich Anmelder

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	38 41 393 C2
DE	196 20 611 A1
DE	196 15 302 A1
US	58 92 904
US	57 90 703
US	57 48 763
US	56 71 282
EP	08 62 318 A2
EP	06 76 877 A2
WO	99 43 167 A1

RULAND,Ch.: Sichere Übertragung und Archivierung elektronischer Dokumente. In: DATACOM 3/91, S.120-130;
KLUTE,Rainer: Verschlußsache. In: iX 12/1995, S.132-145;
STAINO,Rumen: Datensicherheit im Internet: Prinzipien, Möglichkeiten und Grenzen. In: ntz, H.8, 1996, S.32-40;
Telesec - Kommunikationssicherheit, Telekom, Siegen, 1994, S.8,9;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zum Versand authentisierter Informationen in Datennetzen

DE 199 26 783 A 1

DE 199 26 783 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Versand authentisierter Informationen in Datennetzen, wie etwa in öffentlichen Weitverkehrsnetzen (z. B. im Internet).

Datennetze und insbesondere öffentliche Weitverkehrsnetze, wie etwa das Internet stellen ihren Benutzern heute ein Medium zur Verfügung, mit dem sie auf schnelle Art und Weise einen großen Adressatenkreis auf bequeme und schnelle Art erreichen können. Dabei kann diese Kommunikation im wesentlichen auf zwei unterschiedlichen Methoden beruhen.

Zum einen ist es möglich mittels sogenannter e-mail gezielt einzelnen oder auch Gruppen von Benutzern des Datennetzes Informationen zu übermitteln, in dem diese an deren e-mail-Adresse gesendet werden.

Zum anderen kann aber auch ein unbestimmter Adressatenkreis innerhalb des Netzes angesprochen werden. Dies geschieht durch Einstellen der zu übermittelnden (bzw. in diesem Falle besser: zu veröffentlichenden) Information in einen zum Zwecke des Informationsabrufs öffentlich zugänglichen Datenbereich, etwa eine Webseite im Internet.

Beide Übermittlungswege finden in seit jeher bekannten Verfahrensweisen ihr jeweiliges Pendant. So entspricht den modernen technischen Möglichkeiten der e-mail der herkömmliche Postweg, bei dem ein Absender einen an den oder die Empfänger adressierten Brief bzw. Briefe versendet, wohingegen der an einen unbestimmten Empfängerkreis gerichteten öffentlich abrufbaren Information (etwa auf einer Webseite) die herkömmliche Verbreitung durch Rundfunksendung, Fernsehen oder auch Zeitungen bzw. Zeitschriften entspricht.

Ein wesentlicher Unterschied zu diesen herkömmlichen Medien besteht jedoch darin, daß es dem Einzelnen unter Zuhilfenahme der neuen elektronischen Möglichkeiten erheblich leichter fällt, sich an einen großen Empfängerkreis, sei er nun bestimmt oder unbestimmt zu wenden. Dies gilt insbesondere auch im Hinblick auf die Möglichkeit nicht nur regionale, sondern auch überregionale, nationale oder gar internationale Kreise zu erreichen.

Auf den herkömmlichen Informationswegen trifft er hierbei hingegen auf verschiedene Schwierigkeiten.

Will er sich im sogenannten redaktionellen Teil der herkömmlichen Medien an einen unbestimmten Empfängerkreis wenden, so ist er auf die Mitwirkung einer Redaktion angewiesen, die sein spezifisches Anliegen für wichtig genug hält, es in dem von ihr kontrollierten Medium zu verbreiten. Die inhaltliche Kontrolle unterliegt dabei immer der Redaktion.

Alternativ hierzu kann er sich in einer Anzeige oder mit einem zu sendenden Spot an seine Zielgruppe wenden, was jedoch einerseits mit erheblichen Kosten verbunden ist, und im Falle nicht werbender, sondern persönlicher oder politischer Inhalte auch nicht von jedem Medium vorbehaltlos akzeptiert wird.

Will der Sender der Informationen sich auf dem Postwege, der nicht von Medien kontrolliert wird, an eine größere Gruppe von Personen wenden, so bleibt hier nur der Weg einer Massensendung, deren Adressen entsprechend der jeweiligen Zielgruppe kostenpflichtig beschafft werden müssen und die darüber hinaus auch einen weiteren nicht unerheblichen Portokostenaufwand verursacht.

Demgegenüber bieten öffentliche Weitverkehrsnetze wie das Internet dem Benutzer solcher Einrichtungen die inhaltlich unkontrollierte und nur seiner eigenen Verantwortung unterfallende Möglichkeit des Informationsangebotes an jedermann im Wege der Einstellung von Informationsangeboten, die von den anderen Nutzern des Netzes ohne an diese

adressiert zu sein abgerufen werden können.

Aber auch der Weg des adressierten Massenversandes an bestimmte Gruppen von Nutzern wird durch die Verwendung dieser Netze erheblich vereinfacht, da die Kosten, die für einen derartigen e-mail Versand aufgewendet werden müssen weit unter denen einer herkömmlichen Massenpostsendung liegen, da keinerlei Porto anfällt und zudem die Netze selber Interessengruppen (newsgroups) via e-mail zugänglich machen, deren elektronische Anschriften dann nicht mehr im kommerziellen Adressenhandel beschafft werden müssen.

Aufgrund dieser für den Einzelnen durch die Verwendung von Datennetzen gegenüber der bisherigen Situation erheblich herabgesetzten Hindernisse, sich mit seinen persönlichen Nachrichten an ein Publikum zu wenden, tritt jedoch das Problem der Authentizität der solchermaßen verbreiteten Nachrichten stärker als bisher zutage. Während im Falle der herkömmlichen Medien entweder eine inhaltliche Kontrolle durch Redaktionen stattfindet, die eine gewisse Gewähr für die verbreiteten Nachrichten bieten oder aber zumindest die hohen Kosten und die gesetzlich klar geregelten Verantwortlichkeiten eine erhebliche Hürde für die Verbreitung von Falschinformationen darstellen, entfallen diese Sicherungsmechanismen im Falle der Verbreitung von Informationen über Datennetze weitgehend. Gleichzeitig steigt aber das Informationsangebot aufgrund der erleichterten Kommunikationsmöglichkeiten, was darin mündet, daß zwar immer mehr Informationen in Datennetzen verfügbar sind, deren Verläßlichkeit jedoch insbesondere im Falle unbekannterer Informationsanbieter zugleich immer fragwürdiger wird.

Dies gilt, wenn auch im verminderten Maße, grundsätzlich auch für den Fall der Kommunikation von einem Absender an nur einen Empfänger, da auch hier die Schwelle zur Verbreitung unrichtiger Informationen aufgrund der technisch erleichterten Möglichkeiten herabgesetzt wird. Dies gilt insbesondere angesichts der Tatsache, daß es via e-mail naturgemäß leichter fällt über den wahren Absender einer Nachricht zu täuschen, als dies mittels herkömmlicher Post möglich ist, die ja üblicherweise eine Unterschrift trägt.

Zur Lösung dieses Problems existieren eine Reihe von Lösungen, etwa die kryptographische Behandlung abzusendender Nachrichten, die ein Vertrauensverhältnis zwischen Absender und Empfänger hinsichtlich des Zugangs zur gesendeten Information gewährleisten helfen soll oder auch die sogenannte elektronische Unterschrift, die ihren Niederschlag im Signaturgesetz der Bundesrepublik Deutschland gefunden hat, welche auch bei öffentlichem Zugang zur Information selbst die Gewähr über ihren Absender leisten soll. All diese Verfahren vermögen jedoch eines nicht sie bieten unabhängig von der Identität des Absenders keine Gewähr für den Inhalt der Nachrichten. Die inhaltliche Qualität von Informationen hängt nach der Verkehrsauffassung immer mit dem guten Namen des Senders der Information, somit der Informationsquelle zusammen. Dies gilt sowohl für den privaten, wie für den öffentlichen Bereich. Beinahe jedem sind in seinem persönlichen Umfeld andere Menschen bekannt, von denen man meint, daß diesen Menschen zu trauen sei, und damit deren Nachrichten und Informationen, die von diesen Menschen an einen selbst herangetragen werden, als zuverlässig einstuft. Ebenso gilt das Umgekehrte:

Beinahe jeder kann Menschen in seinem Umfeld benennen, die als Schwindler gelten und die so als zuverlässige Informationsquellen untauglich sind. Im öffentlichen Bereich stellt sich diese Situation ähnlich dar: Große bekannte Namen, etwa von Unternehmen oder Institutionen gewährleisten hier Vertrauen in die unter diesen Namen in Verkehr ge-

brachten Informationen. Bekannte Nachrichtenagenturen etwa geben hierfür ein gutes Beispiel. Der sogenannte "gute Name" vermag hier für die Qualität der verbreiteten Information einzustehen. Informationen hingegen, die von Unbekannten dargeboten werden, vermag man nur im verminderten Maße oder im Extremfall gar keinen Glauben zu schenken.

So stehen nun Informationsanbieter, die sich die neuen erleichterten Möglichkeiten der Datennetze zur Informationsverbreitung zu Nutze machen wollen vor einem Problem. Zwar hindert sie einerseits nichts mehr, ihre Informationen anzubieten, andererseits schenkt man ihnen womöglich kein Vertrauen hinsichtlich des Inhaltes dieser Informationen: Ihnen fehlt der gute Name, dem man dies Vertrauen schenken würde! Der Aufbau eines solchen ausreichend bekannten guten Namens jedoch ist schwierig, zeitraubend und kostenintensiv.

Daher ist es Aufgabe der vorliegenden Erfindung ein Verfahren anzugeben, welches es auf technischem Wege ermöglicht, Informationen in Datennetzen anzubieten oder zu versenden, die den Empfängern der Informationen eine Prüfung der Authentizität der Information ermöglicht oder doch zumindest erleichtert.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren zur Authentisierung einer von einem Absender stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern bestimmten Information, die in einem Datennetz versendet oder in ein Datennetz zur Einsichtnahme eingestellt wird gelöst, wobei (i) die vom Absender stammende Information zunächst in einen im Datennetz verkehrsfähigen Code übertragen wird, und (ii) hiernach im Datennetz an bestimmte Empfänger übertragen wird oder in das Datennetz zur Einsichtnahme eingestellt wird und das erfindungsgemäß dadurch gekennzeichnet ist, daß in einem Zwischenschritt nach Schritt (i) und vor Schritt (ii), (i).a) der vom Absender stammenden und bereits codierten Information vor ihrer Versendung im Datennetz oder Einstellung in das Datennetz ein Authentisierungscode hinzugefügt wird, der die Identifikation des Authentisierenden erlaubt.

Auf diese Weise kann als Authentisierender eine Person oder Organisation auftretenden, der über den bereits o. a. guten Namen verfügt, dem der Informationsempfänger zu trauen bereit ist. Der Authentisierende wird seinen guten Namen nicht gefährden wollen und wird seinerseits nur solche Informationen authentisieren, die er in seinem guten Namen zu verantworten glauben kann. Im Extremfall, wo eine besonders hohe Authentizität der Information verlangt wird, ist es dabei z. B. möglich, daß ein Notar die Authentisierung durchführt, der für den Fall einer falschen Authentisierung gegen seine Amtspflichten verstoßen würde.

Dabei kann in dem Verfahren nach der vorliegenden Erfindung auch vorgesehen sein, daß der codierten Information zusätzlich zum Authentisierungscode eine codierte Authentizitätsinformation hinzugefügt wird, in der hinterlegt ist, inwieweit die codierte Information authentisch ist. So ist es beispielsweise einem Notar der als Authentisierender fungiert möglich, zu beglaubigen (authentisieren), daß ein digital codiertes Foto eine bestimmte Person abbildet oder, daß ein bestimmter in der Information wiedergegebener Sachverhalt den Tatsachen entspricht.

Sowohl der Authentisierungscode, als auch die Authentizitätsinformation können neben den Inhalten, die zur Erfüllung ihrer vorgenannten Funktionen erforderlich sind, weitere Zusatzinformationen enthalten. So kann etwa der Authentisierungscode auch auf ein eigenes Informationsangebot des Authentisierenden im Datennetz hinweisen, welches näheren Aufschluß über ihn oder die betreffende Authentisierung gibt.

In einer bevorzugten Ausführungsform des Verfahrens zur Authentisierung einer vom Absender stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern bestimmten Information sind der, der codierten Information zugefügte Authentisierungscode und/oder die hinzugefügte codierte Authentizitätsinformation so ausgestaltet, daß sie eine Kennzeichnung aufweisen, zu deren Benutzung nur der Authentisierende befugt ist. Dabei kann es sich um jegliche Arten von geschützten Kennzeichen wie etwa Marken, Wiedergabe von Siegeln, geschäftliche Bezeichnungen, Titel oder auch urheberrechtlich geschützte Werke handeln. Durch eine solche Aufnahme einer für den Authentisierenden geschützten Kennzeichnung wird rechtlich sichergestellt, daß kein Unbefugter die Informationen authentisiert, da ein solcher zur Verwendung des betreffenden Kennzeichens nicht berechtigt ist.

Eine besonders bevorzugte Ausführungsform des Verfahrens zur Authentisierung einer vom Absender stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern bestimmten Information nach der vorliegenden Erfindung ist dadurch gekennzeichnet, daß der, der codierten Information zugefügte Authentisierungscode und die womöglich hinzugefügte Authentizitätsinformation so ausgestaltet sind, daß sie eine Überprüfung der Zugehörigkeit von codierter Information zu Authentisierungscode und/oder codierter Authentizitätsinformation ermöglichen.

Zur weiteren Verbesserung des Verfahrens nach der vorliegenden Erfindung kommen darüber hinaus auch steganographische Methoden in Frage, wie etwa die Verwendung eines digitalen Wasserzeichens:

In einer solchen Ausführungsform nach der vorliegenden Erfindung kann ein als digitales Wasserzeichen bekanntes Merkmal verwendet werden, das der Information oberflächlich unmerklich im Code hinzugefügt wird, gleichwohl jedoch die Bestimmung ihrer Identität erlaubt. In Kombination mit der Authentizitätscodierung und/oder der Authentizitätsinformation angewandt, ist es so möglich festzustellen, ob Information und Authentizitätscodierung und/oder Authentizitätsinformation tatsächlich zusammengehören oder ob eine Information einer nicht zugehörigen Authentizitätscodierung und/oder Authentizitätsinformation hinzugefügt und somit dem Authentisierenden untergeschoben wurde. Dies kann etwa dergestalt geschehen, daß sowohl die Information selbst, als auch der Authentisierungscode und/oder die Authentizitätsinformation mit dem selben digitalen Wasserzeichen versehen werden.

Ein Test der Zugehörigkeit der Teile zueinander kann dann erfindungsgemäß so erfolgen, daß geprüft wird, ob das der codierten Information hinzugefügte digitale Wasserzeichen identisch mit dem digitalen Wasserzeichen des Authentisierungscodes und/oder der Authentizitätsinformations ist und nur in diesem Falle die Zugehörigkeit zueinander positiv bestätigt wird.

Auch kann der Authentisierungscode als digitale Signatur ausgestaltet sein, die den Authentisierenden als den Inhaber der Signatur identifiziert. So kann der Authentisierende nach Maßgabe etwa des Signaturgesetzes rechtlich eindeutig identifiziert werden, womit seitens der Informationsempfänger Klarheit über die Identität des Authentisierenden besteht. Nach der vorliegenden Erfindung kann die codierte und authentisierte Information dann via e-mail im Internet an einen bestimmten Kreis von Empfängern gesendet werden.

Sie kann aber vorzugsweise auch im World Wide Web des Internet zur Einsichtnahme als Webseite eingestellt werden, wobei die so abzurufenden Informationen nicht nur von einzelnen aktiv hiernach nachfragenden Empfängern empfangen werden können, sondern etwa auch mittels öffentlicher

aufgestellter Monitore oder Bildprojektoren einem Publikum an einem bestimmten Ort angeboten werden können.

Auch ist eine Verknüpfung beider Versandmethoden, also die Methode der Versendung an bestimmte mit der Methode der Versendung an unbestimmte Empfänger möglich, etwa indem in den an bestimmte Empfänger versandten e-mails mit den Informationen ein Hinweis versendet wird (vorzugsweise ein Hyperlink), der auf die gleichfalls in das Datennetz eingestellte Information verweist, die an einen unbestimmten Kreis von Empfängern gerichtet ist.

Eine besonders bevorzugte Ausführungsform des Verfahrens nach der vorliegenden Erfindung ist dadurch gekennzeichnet, daß als Information mindestens eine Bildinformation (Foto) codiert wird, deren Authentizität dann durch den Authentisierenden bestätigt wird. Insbesondere mit Digitalkameras aufgenommene Fotos bieten sich hierzu besonders an, da diese einerseits (z. B. als aktuelles Pressefoto) digital schnell weiter versendet werden sollen und können, zum anderen aber gerade die Glaubwürdigkeit solcher Digitalaufnahmen aufgrund der inzwischen hoch entwickelten Bildbearbeitungstechnik im Computer heute schon oftmals leidet. Selbstverständlich können aber auch herkömmlich aufgenommene und dann gescannte Aufnahmen als zu versendende Information im Sinne der vorliegenden Erfindung verwendet werden. Neben der codierten Bildinformation kann die zu versendende Information natürlich auch noch andere Informationen, wie etwa Texte, vorzugsweise auch Grüße an den Empfänger aufweisen.

Die vorgenannten Verfahren ermöglichen es somit auch unbekannten Informationsanbietern durch technische Maßnahmen, je nach Anforderung auf unterschiedlichem Sicherheitsniveau durch glaubwürdige Dritte authentisierte Informationen zu verbreiten. Im Fall höchster nachgefragter Sicherheit kann hiermit etwa ein Notar unter Verwendung seiner eigenen dem Signaturgesetz entsprechenden digitalen Signatur eine Information eines Informationssenders authentisieren und mit einer eigenen von ihm verfaßten Authentizitätsinformation versehen, wobei die Zugehörigkeit untereinander etwa durch ein digitales Wasserzeichen sichergestellt wird.

Im folgenden werden nicht einschränkend zu verstehende Ausführungsbeispiele anhand der Zeichnung besprochen. In dieser zeigt:

Fig. 1 eine schematische Darstellung zur Erläuterung des Verfahrensablaufs nach der vorliegenden Erfindung.

Fig. 1 zeigt eine schematische Darstellung zur Erläuterung des Verfahrensablaufs nach der vorliegenden Erfindung anhand eines leicht nachzuvollziehenden Beispiels: Ein Absender **1** codiert eine Information **2** und hinterlegt diese in einem Computer **3**. Beipielsweise möchte der Absender die Information **2** versenden, daß er selbst auf einer bestimmten Feier zusammen mit einem Prominenten zugegen war. Von dieser Veranstaltung und seinem Zusammensein mit dem Prominenten dort besitzt er ein Foto, welches dort vorzugsweise mit einer Digitalkamera aufgenommen wurde. Die Glaubwürdigkeit dieses Fotos, das ihn zusammen mit dem Prominenten zeigt, ist jedoch angesichts heutiger digitaler Bildbearbeitungsmöglichkeiten stark eingeschränkt. Dem Absender **1** liegt jedoch daran, daß dieses Foto für authentisch gehalten wird. So bittet er einen Authentisierenden **4**, beispielsweise den bekannten Veranstalter der Feier, dem man die Authentizität des Fotos ohne weiteres abnimmt, darum, die von ihm im Computer 3 codiert hinterlegte Information **2**, also hier das Foto, zu authentisieren, in dem er sein geschäftliches Kennzeichen (z. B. seine Firma oder auch eine Marke seines Hauses, unter der er z. B. die Feier durchgeführt hat) als Authentisierungscode und den Hinweis auf die Echtheit der Abbildung als Authentizitätsinformation der Information **2** hinzufügt, nachdem er sich davon überzeugt hat, daß das Foto **2** mit der Wirklichkeit **5** übereinstimmt. Sodann kann die solchermaßen ergänzte und damit nun authentisierte Information **2a** in ein Datennetz **6**, z. B. das Internet eingestellt werden. Hieraus können dann die Empfänger **7**, diese nun durch das Kennzeichen des Veranstalters **4** authentizierte Information **2a** etwa von einer Webseite abrufen und im Rahmen ihres Vertrauens gegenüber dem Veranstalter **4** und nicht gegenüber dem Absender **1** dem Foto **2a** Glauben schenken. Auf diese Weise kann über jede Information **1** ein gesteigertes Vertrauen im Rahmen der Glaubwürdigkeit des Authentisierenden **4** hergestellt werden. Für das hier genannte Beispiel heißt dies, daß so z. B. auch die Information, daß der Absender **1** überhaupt an einem bestimmten Ort (z. B. der Feier) gewesen ist, im Rahmen der Glaubwürdigkeit des Authentisierenden **4** authentisiert werden kann.

Der Authentisierungscode oder die Authentizitätsinformation können dabei der Verwendung entsprechend zum Gesamtbild der Information passend ausgestaltet werden. Im vorgenannten Beispiel hieße dies etwa, daß diese graphisch als Rahmen rund um das Foto **2** ausgestaltet werden können, wobei auf diesem Rahmen farblich passend abgesetzt das Kennzeichen des Veranstalters **4** und dessen Authentizitätsinformation sprachlich geschickt abgefaßt (etwa in der Art: Dies Foto zeigt Herrn X auf der Feier F) angebracht werden können. Sowohl der Authentisierungscode als auch die Authentisierungsinformation können dabei auch weitere Zusatzinformationen enthalten. So können sie auch auf ein eigenes Informationsangebot des Authentisierenden (**4**) im Datennetz hinweisen oder auf die Feier selbst, und so näheren Aufschluß über die Umstände der betreffenden Authentisierung anläßlich der Feier oder auch die Umstände der Feier selbst geben und so die Glaubwürdigkeit der Information weiter erhöhen. Vorzugsweise sind sie dabei selbst als Hyperlink auf weitere Webseiten ausgestaltet.

Selbstverständlich können derartige Informationen nicht nur im Sinne eines Broadcast (also einer Information die an einen unbestimmten Empfängerkreis gerichtet ist) in ein Datennetz eingestellt werden, sondern natürlich auch an bestimmte Empfänger **7** oder Gruppen von Empfängern **7** z. B. via e-mail gesendet werden.

Patentansprüche

1. Verfahren zur Authentisierung einer von einem Absender (**1**) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (**7**) bestimmten Information (**2**), die in einem Datennetz (**6**) versendet oder in ein Datennetz (**6**) zur Einsichtnahme eingestellt wird, wobei

   (i) die vom Absender (**1**) stammende Information (**2**) zunächst in einen im Datennetz (**6**) verkehrsfähigen Code übertragen wird, und

   (ii) hiernach im Datennetz (**6**) an bestimmte Empfänger (**7**) übertragen wird oder in das Datennetz (**6**) zur Einsichtnahme eingestellt wird,

   dadurch gekennzeichnet, daß in einem Zwischenschritt nach Schritt (i) und vor Schritt (ii),

   (i).a) der vom Absender (**1**) stammenden und bereits codierten Information (**2**) vor ihrer Versendung im Datennetz (**6**) oder Einstellung in das Datennetz (**6**) ein Authentisierungscode hinzugefügt wird, der die Identifikation des Authentisierenden (**4**) erlaubt.

2. Verfahren zur Authentisierung einer vom Absender (**1**) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (**7**) bestimmten Infor-

mation (2) nach Anspruch 1, dadurch gekennzeichnet, daß der codierten Information (2) zusätzlich zum Authentisierungscode eine codierte Authentizitätsinformation hinzugefügt wird, in der hinterlegt ist, inwieweit die codierte Information (2) authentisch ist.

3. Verfahren zur Authentisierung einer vom Absender (1) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (7) bestimmten Information (2) nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der, der codierten Information (2) zugefügte Authentisierungscode und/oder die womöglich hinzugefügte codierte Authentizitätsinformation so ausgestaltet sind, daß sie eine Kennzeichnung aufweisen, zu deren Benutzung nur der Authentisierende (4) befugt ist.

4. Verfahren zur Authentisierung einer vom Absender (1) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (7) bestimmten Information (2) nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, daß der, der codierten Information (2) zugefügte Authentisierungscode und die womöglich hinzugefügte codierte Authentizitätsinformation so ausgestaltet sind, daß sie eine Überprüfung der Zugehörigkeit von codierter Information (2) zu Authentisierungscode und/oder codierter Authentizitätsinformation ermöglichen.

5. Verfahren zur Authentisierung einer vom Absender (1) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (7) bestimmten Information (2) nach Anspruch 4, dadurch gekennzeichnet, daß sowohl die codierte Information (2) selbst als auch der Authentisierungscode und/oder die codierte Authentizitätsinformation mit einem identischen digitalen Wasserzeichen versehen werden.

6. Verfahren zur Authentisierung einer vom Absender (1) stammenden und für einen bestimmten oder unbestimmten Kreis von Empfängern (7) bestimmten Information (2) nach Anspruch 1, 2, 3, 4 oder 5, dadurch gekennzeichnet, daß der Authentisierungscode als digitale Signatur ausgestaltet ist, die den Authentisierenden (4) als den Inhaber der Signatur identifiziert.

7. Verfahren zur Authentisierung einer vom Absender (1) stammenden Information (2) nach Anspruch 1, 2, 3, 4, 5 oder 6, dadurch gekennzeichnet, daß die codierte Information (2) via e-mail im Internet (6) an einen bestimmten Kreis von Empfängern (7) gesendet wird.

8. Verfahren zur Authentisierung einer vom Absender (1) stammenden Information (2) nach Anspruch 1, 2, 3, 4, 5 oder 6, dadurch gekennzeichnet, daß die codierte Information (2) im World Wide Web des Internet (6) zur Einsichtnahme als Webseite eingestellt wird.

9. Verfahren nach einem der Ansprüche 1, 2, 3, 4, 5, 6, 7 oder 8, dadurch gekennzeichnet, daß als Information (2) mindestens eine Bildinformation (Foto) codiert wird.

10. Verfahren zur Überprüfung der Zugehörigkeit von einer codierten Information (2) zu einem Authentisierungscode und/oder einer codierten Authentizitätsinformation, wobei überprüft wird, ob das der codierten Information (2) hinzugefügte digitale Wasserzeichen identisch mit dem digitalen Wasserzeichen des Authentisierungscodes und/oder der Authentizitätsinformations ist und nur in diesem Falle die Zugehörigkeit zueinander positiv bestätigt wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 199 26 783 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 14. Dezember 2000

FIG. 1